

ASSEMBLY, No. 1368

STATE OF NEW JERSEY 222nd LEGISLATURE

PRE-FILED FOR INTRODUCTION IN THE 2026 SESSION

Sponsored by:

Assemblywoman ELLEN J. PARK

District 37 (Bergen)

Assemblyman ROBERT J. KARABINCHAK

District 18 (Middlesex)

Co-Sponsored by:

Assemblymen Clifton and Scharfenberger

SYNOPSIS

Requires certain State employees to receive training in cybersecurity best practices.

CURRENT VERSION OF TEXT

As reported by the Assembly State and Local Government Committee with technical review.



(Sponsorship Updated As Of: 3/9/2026)

1 AN ACT concerning State cybersecurity and supplementing Title 52
2 of the Revised Statutes.

3

4 **BE IT ENACTED** *by the Senate and General Assembly of the State*
5 *of New Jersey:*

6

7 1. As used in this act:

8 a. "State agency" means any of the principal departments in the
9 Executive Branch of the State Government, and any division, board,
10 bureau, office, commission or other instrumentality within or
11 created by such department, the Legislature of the State and any
12 office, board, bureau or commission within or created by the
13 Legislative Branch, and, to the extent consistent with law, any
14 interstate agency to which New Jersey is a party and any
15 independent State authority, commission, instrumentality or agency.
16 A county or municipality shall not be deemed an agency or
17 instrumentality of the State.

18 b. "State employee" means any person holding an office or
19 employment in a State agency, including a member of the
20 Legislature.

21

22 2. Every State employee who has access to a State agency
23 computer shall annually undergo cybersecurity training
24 incorporating best practices as presented by the New Jersey
25 Cybersecurity and Communications Integration Cell, established
26 pursuant to Executive Order No. 178 (2015) in the New Jersey
27 Office of Homeland Security and Preparedness. The office may, in
28 its discretion, make the training available as an online course. The
29 training shall include, but need not be limited to, updating
30 passwords; detecting phishing scams; preventing ransomware,
31 spyware infections, and identity theft; and preventing and
32 responding to data breaches.

33 The Director of the Office of Homeland Security and
34 Preparedness shall adopt guidelines to implement the requirements
35 of this section.

36

37 3. This act shall take effect immediately.